



Department of Homeland Security Daily Open Source Infrastructure Report for 19 December 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Portsmouth Herald reports ISO New England is warning residents that they may have to implement rolling blackouts during the coldest winter months in 2006, and is providing a public-service announcement system letting people know when power demand is high. (See item [1](#))
- The Associated Press reports the University of Illinois has launched a Web log, or blog, for farmers, called Farm Gate, providing information on agricultural topics, ranging from crop science to economics to veterinary medicine. (See item [18](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *December 18, Portsmouth Herald (ME)* — ISO New England issues warning, urges conservation. Power companies across New England are warning residents they may implement rolling blackouts during the coldest winter months in 2006. ISO New England, the nonprofit corporation that coordinates the power grid for the region, has said this winter's electricity demand could set new records, even under normal weather conditions. This, combined with disrupted natural gas supplies in the Gulf of Mexico, could cause a spike in electricity demand. If the demand is too great for the power grid, ISO New England will likely

require companies to cut the power in certain areas of the Northeast. Because ISO New England is powered 40 percent by natural gas, it is concerned about the tight supply, said Ken McDonnell of ISO New England. Home-heating companies typically get the first supplies of natural gas, leaving the rest for power companies. Increase in demand is another concern for ISO New England, having gone up three percent since the record-setting winter of 2004, he said. ISO New England has also created a public-service announcement system in each state, letting people know when power demand is high. These announcements, which ask average energy users to turn off appliances and lights and to avoid doing laundry during early evening hours, have been very successful in the past.

Source: <http://www.seacoastonline.com/news/12182005/maine/78575.htm>

2. *December 17, Salem News (MA)* — **Nuclear plant accident kills one in Russia.** Hundreds of pounds of molten metal splashed from a smelter at a Russian nuclear power plant, killing one worker and severely injuring two others, a scientist and the federal nuclear agency said Friday, December 16. The accident did not affect reactors, the agency said. The mishap occurred at the plant in the closed nuclear town of Sosnovy Bor, 50 miles west of the northern city of St. Petersburg. The smelter is operated by Ekomet-S, a company reprocessing scrap metal. A plant spokesperson said the accident was caused by violations of technical and production rules. The accident on Thursday, December 15, shone a spotlight on what environmentalists called uncontrolled operations at Russian nuclear sites. A 33-year-old worker died of his injuries and two others were injured, said Yuri Lameko, chief doctor of the Sosnovy Bor hospital. This was the second accident at Ekomet-S, with the first happening in summer 2003 and injuring two workers.

Source: <http://www.ecnnews.com/cgi-bin/05/snstory.pl?-sec-News+1k589gO+fn-17russia-20051217->

3. *December 17, News 14 Carolina (NC)* — **Additional power crews helping with ice storm recovery efforts.** Utility crews from 16 states are assisting Duke Power with ice storm recovery efforts. One thousand utility workers came into the area Friday, December 16, and another 1,000 are on the way. The additional manpower, combined with Duke Power's 6,500 employees and contractors, brings the total number of personnel working to restore power to more than 9,000. Duke Power officials said the immediate Charlotte, NC, area is now powered up, but there are still other parts of the region that are in the dark. Power crews have been working around the clock. As of 5:30 p.m. EST Saturday, electricity has been restored to 358,600 customers, but there are still 341,400 reported outages in both North and South Carolina. At the ice storm's peak, there were nearly 700,000 Carolina residents without power

Source: http://www.news14charlotte.com/content/local_news/gaston/?AC=&ArID=109249&SecID=7

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *December 16, Associated Press* — **Hotel evacuated after carbon monoxide leak.** More than 100 guests at a Holiday Inn in Hunterdon County, NJ, were evacuated early Friday morning, December 16, after high levels of carbon monoxide were detected in the building. The guests were taken from their rooms at about 1 a.m. EST and brought to the hotel lobby, where they

were met by emergency medical personnel who checked for signs of carbon monoxide poisoning. Some guests were taken to nearby hospitals as a precautionary measure, said Frank Veneziale, deputy director of the Hunterdon County Office of Emergency Management. Two guests who were taken to Somerset Medical Center were treated and released, said Kathleen Roberts, a hospital spokesperson. At Hunterdon Medical Center, 12 people were treated and released, said hospital spokesperson Kathleen Seelig. The hotel was ventilated by fire department personnel, and guests were allowed to return to their rooms at 3:18 a.m. EST. Veneziale said he did not know what caused the increased carbon monoxide levels.

Source: <http://www.newsday.com/news/local/wire/newjersey/ny-bc-nj--g-as-leak1216dec16.0.5348821.story?coll=ny-region-apnewjersey>

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *December 15, Government Accountability Office* — **GAO-06-222R: Unmanned Aircraft Systems: Global Hawk Cost Increase Understated in Nunn-McCurdy Report (Correspondence).** The Air Force's Nunn-McCurdy report to Congress understates the unit cost increase in that it does not include \$400.6 million in known additional procurement costs.³ Including these costs results in procurement unit cost growth of 31 percent over the current baseline versus the 18 percent reported by the Air Force. In the Government Accountability Office's (GAO) view, this larger unit cost increase should have been reported to Congress with the required certification by the Secretary of Defense. The additional costs not included in the Air Force's reporting are for the purchase and installation of sensors, enhancements to communications equipment and ground stations, parts procurement, and other items required to achieve the system's initial, full-up capability. Air Force Global Hawk program budget documents included these costs before submitting the April 2005 Nunn-McCurdy notice to Congress and before the March 2005 publication of the annual Selected Acquisition Report. GAO believes these costs should have been reported since they are needed to achieve the system's required capabilities. GAO is recommending that the Office of the Secretary of Defense revise the Global Hawk Selected Acquisition Report and take the necessary actions to comply with the Nunn-McCurdy legislation for reporting and certification.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-222R>

[\[Return to top\]](#)

Banking and Finance Sector

6. *December 18, Associated Press* — **Law would catch Internet phishing scammers.** "Phishing" is a computer scam that can quickly drain entire bank accounts of unsuspecting consumers, but it victimizes bigger players, too. Two New York lawmakers want to give legitimate companies whose systems and identities were illegally commandeered to perpetrate such scams the chance to strike back. A bill introduced by state Sen. Charles Fuschillo and Assemblyman Richard Brodsky would allow private companies, nonprofit groups, and the state attorney general to bring civil actions against phishing scam artists. Phishing refers to e-mails that appear to come from banks or other trusted businesses and are used to induce recipients to verify their accounts

by typing personal details, such as credit card or bank account information, into a Website disguised to appear legitimate. "Banks and Internet companies whose names are being used in these scams are as much a victim as the person whose identity is stolen," said Brodsky.

"Companies like Microsoft could very effectively on a civil basis use their muscle to police the system." Nationwide in 2004, 2.4 million were victims of phishing scams costing nearly one billion dollars, said Fuschillo. At least 11 other states enacted anti-phishing legislation in the past year, according to the National Conference of State Legislatures.

Source: <http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--internetphishing1218dec18.0.3104539.story?coll=ny-region-apnewyork>

7. *December 16, eWeek* — **Phishing attack targets credit unions.** Malicious hackers are targeting U.S. credit unions with phishing e-mails that try to take advantage of a recently patched Internet Explorer browser hole to compromise systems used by the bank, according to Credit Union Information Security Professionals Association (CUISPA), an association of IT professionals who work at credit unions. The attacks use e-mail messages that are being sent to CEOs and other executives at credit unions across the U.S. The messages contain a link to a Web page that, when visited, attempts to download a Trojan horse program onto the executives' machines. Beginning on Monday, December 12, executives at the banks began receiving identical e-mail messages with the subject "Credit Union." The messages provide the URL of a Web page that appears to be a credit union "affiliated" with the recipient's bank. The message asks the recipient to help confirm that the credit union is a federally recognized institution, according to a copy of the message posted by CUISPA on its Website. Executives who clicked on the link were taken to a Web page that attempted to download two pieces of malicious code on their machines. One was a Trojan horse program called "Bloodhound.Exploit.54" that uses a recently discovered hole in IE.

Source: <http://www.eweek.com/article2/0,1895,1902896,00.asp>

8. *December 16, Associated Press* — **Treasury changes money laundering rules.** The U.S. Treasury Department has finalized rules requiring banks, securities dealers, and other financial institutions to take steps to detect money laundering or other dubious transactions in accounts they maintain for foreign customers. The department's Financial Crimes Enforcement Network on Friday, December 16, announced the new provisions aimed at thwarting terrorist financiers, drug lords, and other money launderers from using the U.S. financial system to carry out financial crimes or conceal illicit activities. The 2001 USA Patriot Act required the department to implement rules governing foreign "correspondent" accounts and private banking. Foreign banks and other financial institutions set up correspondent accounts with U.S. banks to conduct business in this country. The final rules require U.S. financial institutions to conduct due diligence on these accounts. At a minimum, U.S. financial institutions must assess the money laundering risks posed by these accounts, put procedures in place to detect money laundering, and periodically review activity in these accounts. In addition, the final rules require U.S. financial institutions to give close scrutiny to accounts held by foreign senior political officials — as well as family members and close associates of those political figures.

Financial Crimes Enforcement Network: <http://www.fincen.gov/>

Source: http://seattlepi.nwsource.com/national/1152AP_Money_Laundryng.html

[[Return to top](#)]

Transportation and Border Security Sector

9. *December 17, Miami Herald (FL)* — **Transportation Security Administration reduces number of screeners at Miami International Airport.** The Transportation Security Administration (TSA) is reducing the number of screeners at Miami International Airport (MIA) to put MIA in line with similar airports. Security checkpoint lines at Miami International Airport could get longer because the Transportation Security Administration recently began cutting 230 full-time screener positions from the airport. The TSA, which had about 1,700 passenger and luggage screeners this summer at MIA, decided it could make do with less. The federal agency studied the airport's layout and passenger counts and concluded that a reduction would put MIA in line with similar airports nationwide. The decision worries airport officials and members of the Miami–Dade Congressional delegation, who fear delays will frustrate passengers. They are lobbying the federal government to reverse its decision. The reductions, which started about a month ago, come as MIA prepares to open in late summer 2006 the South Terminal, which will have three new security checkpoints. Airport officials noted Miami International handles the third–most international travelers of American airports. Lauren Stover, TSA's spokesperson in Miami, said the cuts could be restored if delays increase. Source: http://www.miami.com/mld/miamiherald/business/13426706.htm?source=rss&channel=miamiherald_business
10. *December 17, Federal Computer Week* — **Border surveillance tech needs improvement, according to Inspector General.** Despite spending more than \$400 million since 1997 on remote surveillance cameras and sensors along U.S. borders, the technology doesn't integrate well and is largely ineffective in detecting illegal activity, according to a new report by the Department of Homeland Security's (DHS) inspector general. The report states that the cameras and seismic and magnetic sensors, which are widely deployed to detect activity along U.S. borders, aren't automatically linked and cover only about five percent of the borders. Along U.S. borders, about 90 percent of the responses to sensor alerts resulted in false alarms, "meaning that [Border Patrol] agents spent many hours investigating legitimate activities," the report adds. Other low-tech methods, such as observations by citizens, Border Patrol agents, and other agency workers, produced a greater percentage of apprehensions than the use of sensors did. The new report provides seven recommendations to help the Border Patrol office, which is part of DHS's Customs and Border Protection agency. The recommendations include improving technology integration and deployment, implementing performance measures, standardizing data collected by the technology, and deploying more mobile surveillance detection systems. Report: http://www.dhs.gov/interweb/assetlibrary/OIG_06-07_Nov05.pdf Source: <http://www.fcw.com/article91756-12-16-05-Web>
11. *December 16, KOCO (OK)* — **Student arrested at Oklahoma City airport after attempted security breach.** An international student at the University of Central Oklahoma (UCO) was arrested Thursday, December 15, at Will Rogers Airport after trying to get through security without a ticket, abducting a woman outside the airport, and then attempting to steal a car, according to police. Humberto Deita, 21, from Puebla, Mexico, and enrolled at UCO, was charged with auto burglary and attempted abduction. Police have not identified exactly what Deita's intent was. Source: http://news.yahoo.com/s/koco/20051217/lo_koco/3128994

12. *December 16, USINFO* — Portugal implements cargo container security initiative. Lisbon, Portugal, has become the latest port to implement the Container Security Initiative (CSI), a screening and inspection program aimed at securing maritime cargo shipments against the threat of terrorism. Lisbon is the 42nd port worldwide to implement the initiative, according to U.S. Customs and Border Protection (CBP) acting Commissioner Deborah J. Spero and Portugal Director-General for Customs and Excise Ana Maria Jordão. Under the security initiative, signed July 7, CBP officers work in partnership with Portuguese customs officials to screen cargo containers headed for the United States that are identified as a potential terrorist risk. To date, 25 customs administrations have committed to join CSI and are at various stages of implementation, according to CBP. "The CSI is a deterrent to terrorists seeking to use containerized cargo as a conduit for terrorism within the maritime environment. Having CSI ports, such as the one in Lisbon, is making U.S. borders more secure and more efficient," said Acting Commissioner Spero. CBP's goal is to have 50 operational CSI ports by the end of 2006. At that time, approximately 90 percent of all transatlantic and transpacific cargo imported into the United States will be subjected to pre-screening.
Source: <http://usinfo.state.gov/eur/Archive/2005/Dec/16-183495.html?chanlid=eur>

13. *December 16, Associated Press* — Officials urge creation of new port of entry. Congestion at the two San Diego-Tijuana border crossings is so great that a new port of entry is needed immediately, officials from both sides of the U.S-Mexico border said. The soonest one can be built, however, is 12 to 14 years away, they said. At a forum at Southwestern College in Chula Vista, CA, put on Thursday, December 15, by the Otay Mesa Chamber of Commerce and the Tijuana Maquiladora Association, U.S. and Mexican federal, state, and local officials outlined the steps being taken and the many more still needed to create a third area border crossing. Application for a presidential permit, which is key to moving the project forward in the United States, was first submitted in February 2001. Ten U.S. federal agencies, 13 Mexican federal agencies, and numerous state and local authorities on both sides of the border must sign onto the plan for it to move forward.
Source: <http://www.nbcsandiego.com/news/5556786/detail.html?rss=dgo&psp=newshttp://www.dot.gov/affairs/dot18205.htm>

14. *December 16, Richmond Times-Dispatch (VA)* — Airport will add part-time screeners. Richmond International Airport (RIA) in Virginia will be a testing ground for part-time federal security screeners early next year. The program, announced by Representative Eric I. Cantor, (R), is meant to help the Transportation Security Administration (TSA) enlarge its screening force at Richmond's fast-growing airport while keeping the government's costs down. TSA director Kip Hawley told Cantor in a letter that Richmond International "is a prime candidate due to peak flight-scheduling" that is, most of its flights leave early in the morning or late in the day, serving a large number of business travelers. The TSA will start recruiting part-time workers in January and February, and hopes to attract younger workers with tuition assistance and lure retired workers with medical benefits. Richmond is part of a broader effort by the TSA to create a national staff in which 20 percent work part time, he said. RIA officials also are pleased that airport security staffing will be reviewed twice a year — a new commitment by the TSA.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1128768751888

15. *December 16, Associated Press* — **Jet evacuated at airport over bomb remark.** A Southwest Airlines jet was evacuated Friday, December 16, on a taxiway after flight attendants overheard a comment about a bomb, but a search of the plane found nothing. Southwest Flight 2074 was preparing to take off from Bob Hope Airport for Las Vegas with about 130 passengers when the pilot taxied to a remote part of the airfield and ordered passengers to evacuate the Boeing 737. One passenger was removed in handcuffs. The others evacuated using a mobile staircase brought to the jet's rear door, said Jennifer Peppin, a spokesperson for the Transportation Security Administration (TSA). She said federal officials did not believe the bomb comment was a credible threat, but authorities questioned five men as a precaution. One was detained. Source: <http://www.msnbc.msn.com/id/10500963/from/RSS/>

[[Return to top](#)]

Postal and Shipping Sector

16. *December 18, NBC 6 News (TX)* — **Suspicious substance found at Temple post office.** Temple, TX's main post office was closed down after a suspicious substance was discovered on a mailbox Friday, December 16. Firefighters and Hazmat technicians were called in to secure the area. Hazmat personnel determined the substance was not a threat, but was Epson Salt. The fire department says Hazmat crews were called in because they didn't know what the substance was, and were worried it might be hazardous. Source: <http://www.kcentv.com/news/c-article.php?cid=12&nid=50>

[[Return to top](#)]

Agriculture Sector

17. *December 16, Casper Star-Tribune (WY)* — **Brucellosis appears in Idaho cattle.** Idaho animal health officials have sent two eastern Idaho beef cattle herds to slaughter due to brucellosis infections and are awaiting word from federal officials as to whether the state will lose its brucellosis-free status. In October, the Idaho Department of Agriculture quarantined a ranch in eastern Idaho's Swan Valley after veterinary medical officers identified a possible case of brucellosis in cattle. Further testing of the herd found a total of eight brucellosis reactors and two additional suspects in the herd. Last week, all 39 cows, two bulls and a few heifer calves were sent to slaughter to end the risk of transmission. John Chatburn, Idaho's deputy administrator for animal industries, said that traceout from that herd found six other animals that had left the herd and were sold through livestock markets. These animals were also taken to slaughter, he said. One of the animals was a 2005 heifer calf that was a brucellosis reactor. The heifer had been placed in a small feedlot with 17 other cattle. This small bunch of cattle was depopulated as well, Chatburn said. Source: <http://www.casperstartribune.net/articles/2005/12/16/news/wyoming/e0c4de28f1cf7a4c872570d800766460.txt>

18. *December 16, Associated Press* — **University of Illinois launches Web log for farmers.** The Internet provides farmers a wealth of information on crop marketing, financial management,

and dealing with crop diseases. But on a busy farm, it can be hard to find time to search the Web for useful information. "We need someone to sort through some of this and put it in a nice logical manner where a farmer can look through it instead of looking all over the Web," said Chris Hausman, who runs a 1,300-acre farm near Champaign. University of Illinois Extension is taking on that challenge with a new blog for farmers. The Farm Gate began publishing earlier this fall and was announced this month. It aims to be a place farmers can go to find information on agricultural topics, ranging from crop science to economics to veterinary medicine. The blog also includes links to other university Websites, extension services in other Midwest states, and other selected agriculture Web pages.

Farm Gate: <http://www.farmgate.uiuc.edu/>

Source: <http://abcnews.go.com/Business/wireStory?id=1412224>

- 19. *December 15, Knight Ridder Newspapers* — Report warns of citrus canker spreading in wake of hurricane.** The winds from Hurricane Wilma may have spread citrus canker so widely that it could result in the destruction of as many as 170,000 more acres of fruit trees in commercial groves, Florida citrus officials said Thursday, December 15. The estimate is based on a preliminary study given to state and citrus industry leaders this week by the U.S. Department of Agriculture (USDA). "I was stunned," said Craig Meyer, Florida's top citrus canker-eradication official. He heard the news at a meeting of growers and state and federal eradication specialists. If the report's predictions come true, millions more trees will have to be destroyed through the eradication program because they are either infected or stand within 1,900 feet of an infected tree. Meyer said the USDA preliminary study suggests that the spread at worst may force the state to take out anywhere from 70,000 to 170,000 additional acres of citrus fruit south and east of Lake Okeechobee. That would raise to about 265,000 the number of acres that must be bulldozed. There are about 750,000 commercial acres of citrus in the state now. Any disease spread by the hurricane that hit Florida on October 24 will not start showing up on trees until early next year.

Source: <http://www.bradenton.com/mld/bradenton/news/nation/13417502.htm>

- 20. *December 09, Purdue University* — Researchers say purple deadnettle harbors soybean cyst nematode.** Purdue University researchers have discovered that a winter weed common throughout Indiana will facilitate reproduction and population increases of soybean cyst nematode (SCN) even when soybeans are not present in the field. Purple deadnettle is a winter annual weed that usually emerges after harvest, overwinters as a seedling and fully develops in the spring. Purdue researchers discovered that SCN's use the purple deadnettle as an alternative host for feeding and reproducing when soybeans haven't been planted. Additional research is being done to determine if juvenile soybean cyst nematodes can last through the winter in the weeds' roots. "SCN infests purple deadnettle roots, just like they do on a susceptible soybean variety," said Bill Johnson, an associate professor of weed science. Soybean cyst nematode has been detected in 82 of the state's 92 counties. Johnson said that two to four million acres in Indiana have been affected. To protect soybean plants from this pest, researchers are trying to find the best timing to control purple deadnettle to reduce soybean cyst nematode densities.

Soybean cyst nematode information: <http://nematode.unl.edu/scn/scnisu.htm>

Source: <http://news.uns.purdue.edu/html3month/2005/051209.Johnson.SC N.html>

[[Return to top](#)]

Food Sector

21. *December 16, Associated Press* — **First shipment of U.S. beef reaches Japan.** The first shipment of U.S. beef in nearly two years arrived in Japan Friday, December 16, after the easing of an import ban put in place amid concerns about mad cow disease, Japan's Health Ministry said. An agricultural organization said, meanwhile, that Japanese beef exports to the U.S. would also resume shortly. Japanese beef was banned four years ago over similar mad cow concerns. Japanese inspectors planned to check the shipment of about 4.6 tons of meat to see that it met government safety guidelines, quarantine official Yuji Kitayama said. They planned to confirm the age of the cows and ensure that the meat doesn't contain material from brains, spinal cords, or other suspect parts. Japan banned on imports of American beef in December 2003 after the first case of mad cow disease was reported in the U.S. After two years of negotiations, Tokyo opened its doors Monday, December 12, to meat from U.S. cows younger than 21 months.

Source: <http://www.macon.com/mld/macon/news/world/13417983.htm>

22. *December 13, University of Wisconsin–Madison* — **New technologies target food–borne illnesses.** In 2000, University of Wisconsin–Madison made a commitment to help tackle food–borne illness this complex problem by hiring an interdisciplinary group of researchers with expertise in food safety. One member of the food safety team now holds patents for two devices that harness cold plasma to kill food–borne pathogens. One device looks like a sandwich–sized block of white ceramic. One side features over 200 circles, arranged in a grid. Each circle houses an electrode, and when the reactor is on, they all work together to produce a constant and uniform flow of plasma. The reactor can be suspended, electrodes pointing downward, above any surface in need of disinfection, such as a moving conveyer belt. The second device decontaminates water and other fluids. The device looks like a large glass jug that holds about one liter, fitted with specialized caps that house the electrical gadgetry needed to produce a plasma. As liquids swirl inside the reactor, cold plasma inactivates the contaminants. Researchers found that within 20 seconds, the reactor inactivates high concentrations of bacteria, killing up to 100,000 colony–forming units per milliliter of liquid.

Source: <http://www.news.wisc.edu/11955.html>

[[Return to top](#)]

Water Sector

23. *December 16, BBC News* — **Toxic leak reaches Russian river.** A toxic river spill from a chemical explosion in China has reached Russian waters, Moscow has said. Russian Emergencies Minister Sergei Shoigu said checks carried out in the Amur river so far showed toxicity levels to be normal. He said arrangements were in place to purify water, and new wells had been drilled to ensure safe supplies. The 100–ton spill is expected to reach the main city in the area, Khabarovsk, in four to five days. Chinese media reported that the spill had significantly diluted in the Songhua River before entering the Amur. About 50 ton of chemicals have been flown in to treat the benzene in the water upstream of Khabarovsk, which has 600,000 inhabitants. Shoigu said the city's central water system would be switched off only in "extreme circumstances". The leak has been flowing down the Songhua River in China

following the blast at a petrochemical plant on November 13 in the city of Jilin. The spill affected the city of Harbin's 3.8 million population, who endured five days with no running water.

Source: <http://news.bbc.co.uk/2/hi/europe/4534542.stm>

24. *December 16, Los Angeles Times (CA)* — **Reservoirs banned as tap water source.** New federal water quality rules are forcing Los Angeles, CA, to take its historic network of reservoirs out of use, ultimately costing the city water department billions of dollars and changing the way it stores and distributes water. Most reservoirs in the country are filled with untreated water and will not be similarly affected. The rules, which tighten standards for disinfection byproducts, are expected to cause about 70 percent of the nation's water systems to change their treatment methods, either by using less chlorine or by switching to methods that don't rely on chlorine. The Metropolitan Water District of Southern California is embarking on an \$856-million conversion of its five treatment plants to use ozone instead of chlorine to purify drinking supplies. Two plants have already made the switch and the others will make the change by 2010. In Los Angeles, which operates the largest open-reservoir system of treated water in the country, the regulations are having a much more tangible effect. To make up for the lost reservoir storage, the city is building underground tanks, installing larger-capacity distribution pipes and routing water directly from its main treatment plant in Sylmar to customers. All told, the work will cost an estimated \$3.5 billion, Parekh said.
- Source: <http://www.latimes.com/news/local/politics/cal/la-me-water16dec16.1.7902557.story?coll=la-news-politics-california>

[[Return to top](#)]

Public Health Sector

25. *December 16, Reuters* — **Local tests show bird flu killed Indonesian man.** A 39-year-old Indonesian man has died from the H5N1 strain of bird flu according to local tests, Health Minister Siti Fadillah Supari said on Friday, December 16. Supari told reporters the ministry was awaiting confirmation of the results from a Hong Kong laboratory affiliated with the World Health Organization (WHO). Indonesia has had nine deaths from bird flu confirmed by the Hong Kong laboratory and five cases where patients have survived. WHO spokesperson Maria Cheng said the victim was from south Jakarta and the initial indications were that it was another isolated case. "There were reports of sick and dying poultry in the neighborhood, so it does look as if there is an identifiable source of exposure," said Cheng.
- Source: <http://www.alertnet.org/thenews/newsdesk/JAK30686.htm>

26. *December 15, Howard Hughes Medical Center* — **How Rickettsial pathogens break into cells.** New research by a team of scientists in France and the U.S. has identified both the receptor proteins that enable *Rickettsia conorii*, the Mediterranean spotted fever pathogen to enter cells. Understanding how this bacterium interacts with the cells of its host could lead to new therapeutic strategies. *Rickettsia* bacteria are transmitted by fleas, ticks, and lice to humans and other mammals, where they can cause dangerous and sometimes fatal infections. *Rickettsia* have been classified by the National Institute of Allergy and Infectious Diseases (NIAID) as agents with potential for use as tools for bioterrorism. Researchers demonstrated that the Ku70 protein on the surface of host cells is critical for *R. conorii* to enter the cell, making it the first

Rickettsial receptor ever identified. The researchers found that *R. conorii* specifically binds to Ku70, and that binding and recruitment of Ku70 at the surface of the host cell are important events in *R. conorii*'s invasion of mammalian cells. In addition, since Ku70 has previously been shown to control cell death, the new findings suggest that *Rickettsia*, which—like several other intracellular parasites—prevent cell death in order to multiply inside living cells, may also use this property of their receptor for a successful infection.

Rickettsial information: http://www.cdc.gov/ncidod/diseases/submenus/sub_rickettsial.htm

Source: <http://www.hhmi.org/news/cossart20051216.html>

27. *December 15, Interfax (Russia)* — **Bird flu still present in three Russian villages.** Bird flu cases remain in three Russian settlements, the Russian Agriculture Ministry reported, quoting Russian Agricultural Control Service data. The settlements are located in the Kurgan and Astrakhan regions and Kalmykia. During the bird flu epidemic, bird flu cases were confirmed in over 60 settlements in nine Russian regions. Bird flu cases among domestic birds were believed to exist in over 90 settlements.

Source: http://www.interfax.ru/e/B/politics/28.html?id_issue=1143640_5

28. *December 15, New England Journal of Medicine* — **Influenza-associated deaths among children in the United States, 2003–2004.** During the 2003–2004 influenza season, researchers requested that state health departments report any death associated with laboratory-confirmed influenza in a U.S. resident younger than 18 years of age. Case reports, medical records, and autopsy reports were reviewed, and available influenza-virus isolates were analyzed at the U.S. Centers for Disease Control and Prevention. One hundred fifty-three influenza-associated deaths among children were reported by 40 state health departments. The median age of the children was three years, and 96 of them were younger than five years old. Forty-seven of the children died outside a hospital setting, and 45 died within three days after the onset of illness. Bacterial coinfections were identified in 24 of the 102 children tested. Thirty-three percent of the children had an underlying condition recognized to increase the risk of influenza-related complications, and 20 percent had other chronic conditions; 47 percent had previously been healthy. The mortality rate was highest among children younger than six months of age. Researchers concluded a substantial number of influenza-associated deaths occurred among U.S. children during the 2003–2004 influenza season. High priority should be given to improvements in influenza-vaccine coverage and improvements in the diagnosis and treatment of influenza to reduce childhood mortality from influenza.

Source: <http://content.nejm.org/cgi/content/short/353/24/2559>

29. *December 14, Yale University* — **Genetic clues to *Sodalis* deepens knowledge of bacterial diseases.** By sequencing the genome of the symbiotic bacterium *Sodalis*, which lives off the major disease-transmitting insect, the tsetse fly, researchers at Yale School of Medicine have come a step closer to understanding how microbial pathogens cause disease. The study looked at the genome in *Sodalis*, the second of three kinds of bacteria known to aid the tsetse fly in feeding off the blood of its host. The tsetse fly is one of many eukaryotes (animals) that live in association with symbiotic microbes or bacteria. These animals depend on the microbes for vital nutrients they can't otherwise produce. When the team sequenced the bacterial genome, they found the hallmarks of an organism transitioning from a free-living state to a symbiotic state. The researchers found that the genome itself, in terms of physical structure and size, looks similar to free-living bacteria. As relationships become symbiotic—more and more dependent

on the host—bacterial genomes usually begin to shrink, but in the case of *Sodalis*, it is the same size as the free-living bacteria. It has the largest number of pseudogenes, products with no function, of any bacteria to date.

Source: <http://www.yale.edu/opa/newsr/05-12-14-03.all.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

30. *December 15, San Diego Union-Tribune (CA)* — Fire crews, deputies test readiness for train disasters. On Tuesday, December 13, a mock fire broke out on a Coaster train in Cardiff, CA, as part of a drill to assess readiness for train disasters. For more than two hours, firefighters from nine North County, CA, departments coordinated to rescue passengers from the disabled train. At the same time, sheriff's deputies joined police officers from Carlsbad and Oceanside to practice subduing a violent attacker loose on the train. "Everything considered,...it went reasonably well," said Jack Glassford, a spokesperson for the Encinitas Fire Department. He said 40 to 50 firefighters from Encinitas, Carlsbad, Oceanside, Del Mar, Vista, San Marcos, Elfin Forest, Escondido and Camp Pendleton participated. Lt. Don Fowler of the Encinitas sheriff's station said officers practiced four scenarios involving the attacker, including one in which the bad guy took a firefighter hostage and tried to escape in the firefighter's uniform. Sarah Benson, a spokesperson for the North County Transit District said the Federal Railroad Administration requires the district to conduct such drills every two years. "It's important for us to expose the fire departments and police departments to the various ins and outs of the train," Benson said, including breaking open car windows.

Source: <http://www.signonsandiego.com/news/northcounty/20051215-9999-1mi15drill.html>

31. *December 15, Government Technology* — Report: Topoff exercise would benefit from effective information sharing. The federal government's biennial Top Officials exercise for homeland security would be more effective if IT systems were developed to track and share information more openly and efficiently among participating agencies and with the private sector, according to a new report from the Homeland Security Department Inspector General Richard Skinner. The report evaluates the Topoff 3 exercise conducted in April 2005 that simulated a pneumonic plague outbreak in Union and Middlesex counties in New Jersey and a mustard gas attack in New London, CT. Overall objectives for the drill were met, the inspector general concluded, but "there is room for improved coordination." Among the shortcomings was participants' lack of understanding of the National Response Plan and the National Incident Management System. In the area of information sharing, Topoff 3 exposed several deficiencies. The secured messaging system and information-reporting structure was insufficient, the inspector general said. Also, there was no standard format for collecting and reporting and no mechanism to determine when and if mission assignments were processed. The inspector general recommended that the executive director of the Office of State and Local Government

Coordination and Preparedness design an information management system for future exercises to make information sharing more standardized and efficient.

Skinner's report: http://www.dhs.gov/interweb/assetlibrary/OIG_06-07_Nov05.pdf

Source: http://www.washingtontechnology.com/news/1_1/daily_news/2761_1-1.html

- 32. *December 15, News-Sentinel (IN)* — Indiana's disaster plan includes backup options.** Local law enforcement officials say although it's unlikely a disaster the magnitude of Hurricane Katrina would strike Allen County, IN, they nonetheless are trying to avoid the communications meltdown that plagued the Gulf Coast afterward. Steve Stone, a spokesperson for the Allen County Sheriff's Department, said a disaster plan for Allen County exists that includes backup options involving mobile "suitcase" communications systems. The county has six self-contained suitcase systems that are kept in a secure location. "If the dispatch center or the City-County Building blew up they'd still be up and running," he said. "It's a laptop computer that works like a phone, and you can plug into the system to make a mobile dispatch." But that represents a last resort. A Disaster Communication Response B.E.S.T. Team (Building Excellent Services through Teams) is examining the effectiveness of the county's public safety communications system. Recommendations for improvement were delivered to Mayor Graham Richard Thursday, December 15. Beyond Allen County, Project Hoosier SAFE-T, a statewide wireless public safety communications system being built in Indiana, is designed to provide a uniformly accessible way for state agencies to communicate using a network of towers. The system should be in place sometime in 2007.

Source: http://www.fortwayne.com/mld/newssentinel/news/local/1341407_7.htm

[[Return to top](#)]

Information Technology and Telecommunications Sector

- 33. *December 16, BBC News (United Kingdom)* — Google, Microsoft, and Sun fund Internet research lab.** Archrivals Google and Microsoft are collaborating to fund research that aims to make the Internet easier to run. Along with Sun Microsystems, the companies are contributing to the \$7.5 million running costs of the Reliable, Adaptive and Distributed Systems Lab. A five-year project at the University of California-Berkeley, the new lab will aim to create software that automates the administration systems for Web services and e-commerce sites. Any software created by the lab's students will be given away freely. Using a technique known as statistical learning the Rad Systems Lab will try to automate many day-to-day administration jobs. Google, Microsoft and Sun are contributing to the lab because all three have enormous data operations that currently demand huge numbers of people to keep running. The development of the software powering these huge operations typically takes place in a very haphazard fashion. The lab aims to replace the patched up programs with more formally tested software that does the same job with far less human oversight. By making it easy to set up and run Web-wide services, the lab also hopes to remove the technology barriers that prevent new competitors from taking on giants such as Microsoft, Yahoo, Google and Amazon.

Source: <http://news.bbc.co.uk/1/hi/technology/4534398.stm>

- 34. *December 16, Government Computer News* — National Institute of Standards and Technology chooses minutia for HSPD-12 biometric standard.** After nearly a year in the making, the National Institute of Standards and Technology (NIST) has been convinced that

minutia is an acceptable way to store fingerprint biometric data on smart cards. Amid pressure from industry, agencies and the administration, NIST Thursday, December 15, released the biometric specification for Federal Information Processing Standard 201, Personal Identity Verification under Homeland Security Presidential Directive 12, calling for agencies to store two index fingerprints on the smart card using the International Committee for Information Technology Standard 358 for minutia. Each fingerprint template shall be wrapped in the Common Biometric Exchange Formats Framework structure, NIST said in Special Publication 800-76. NIST originally wanted to store fingerprints using a digital image because it is more entrenched, while minutia is still new and the standard hasn't been tested enough. During the past 11 months, the indecision caused the White House to get involved in the final decision. Agencies, vendors and other interested parties have until January 13, 2006, to comment on this latest draft. NIST then will issue a final version about a month later.

Federal Information Processing Standards Publication on Personal Identity Verification of Federal Employees and Contractors:

<http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf>

NIST Special Publication 800-76:

http://csrc.nist.gov/publications/drafts/800-76Draft/sp-800-76_draft.pdf

Source: http://www.gcn.com/vol1_no1/daily-updates/37790-1.html

35. *December 14, Network World* — **AT&T launches 24-hour security news service.** AT&T Wednesday, December 14, turned on a 24-hour security news service that streams to customers of the carrier's Internet Protect service. The always-on Webcast includes regular programming that is interrupted by security alerts that AT&T deems important enough to let customers know about right away. "We're building a security geek channel," said AT&T CSO Ed Amoroso during his keynote address at Interop New York, during which he announced the service. Programming includes lectures on technologies, interviews with corporate CIOs as well as twice-daily news updates. The alerts will call attention to worms and viruses and suggest ways to deal with them, Amoroso says. These supplement the existing alerts that AT&T would send along as part of Internet Connect. Amoroso acknowledged that most threats come from inside corporate networks, and he characterized badly written software as the biggest threat to network security, but he said AT&T's service could help deal with threats coming from outside.

Source: <http://www.networkworld.com/news/2005/121405-att-security.ht ml>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of malicious software exploiting a vulnerability in the Microsoft Distributed Transaction Coordinator (MSDTC). Successful exploitation could allow a remote, unauthenticated attacker to execute arbitrary code on the system. US-CERT is also aware of increased scanning activity on port 1025/tcp, a port commonly used by this service. For more information about this vulnerability can be found in the following US-CERT

Vulnerability Note:

VU#180868 Microsoft Distributed Transaction Coordinator vulnerable to buffer overflow via specially crafted network message please see vulnerability note: <http://www.kb.cert.org/vuls/id/180868>

Microsoft has released an update to address this vulnerability in Microsoft Security Bulletin MS05-051 please see: <http://www.microsoft.com/technet/security/Bulletin/MS05-051.msp>

US-CERT encourages administrators to apply the appropriate updates as soon as possible.

Exploit for Vulnerability in Microsoft Internet Explorer window() object US-CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles requests to the window() object. If exploited, the vulnerability could allow a remote attacker to execute arbitrary code with the privileges of the user. Additionally, the attacker could also cause IE (or the program using the WebBrowser control) to crash. According to Microsoft, malicious software is targeting this vulnerability. We have confirmed that the proof of concept code is successful on Windows 2000 and Windows XP systems that are fully patched as of November 30, 2005. For more information about this vulnerability can be found in the following US-CERT Vulnerability Note:

VU#887861 Microsoft Internet Explorer vulnerable to code execution via mismatched DOM objects. <http://www.kb.cert.org/vuls/id/887861>

Microsoft has released an update to address this vulnerability in Microsoft Security Bulletin MS05-054. <http://www.microsoft.com/technet/security/bulletin/ms05-054.msp>

US-CERT encourages administrators to apply the appropriate updates, patches, or fixes as soon as possible.

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 6346 (gnutella-svc), 445 (microsoft-ds), 4142 (oidocsvc), 6881 (bittorrent), 27015 (half-life), 25 (smtp), 32789 (---), 80 (www), 135 (epmap) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

December 16, St. Louis Business Journal — **Missouri governor calls on agency to study dam safety law.** Missouri Governor Matt Blunt is calling on the state's Department of Natural Resources to take a comprehensive study of Missouri's dam safety law and compare it to other states. The order comes two days after a reservoir at the Ameren Corp.'s Taum Sauk Hydroelectric Plant ruptured, spilling 1.5 billion gallons of water into the surrounding area in minutes and damaging parts of Johnson's Shut-In State Park near Lesterville, MO. Ameren officials said they believed the breach was about 600 feet long. The department regulates and inspects 653 dams in the state, and said all are in compliance. It also encourages dam owners to inspect their dams regularly. The state does not inspect hydroelectric dams, including Taum Sauk, which are regulated by the Federal Energy Regulatory Commission.

Source: <http://biz.yahoo.com/bizj/051216/1204758.html?.v=1>

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:
<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.